Amendments to the Claims:

Below is a listing of all claims using a strikethrough and underlining to show changes.

1. (currently amended) A secure credit card, comprising:

a) a counter;

b) a pseudo-random bit sequence generator;

c) a clock for driving the counter and for driving the pseudo-random bit sequence generator, wherein the clock is operable for an unpredictable number of cycles, wherein the unpredictable number of cycles is determined by a human action of unpredictable duration.

2. (original) The secure credit card of claim 1 wherein the counter is a first linear feedback shift register (LFSR).

3. (original) The secure credit card of claim 2 wherein the first LFSR has a different initial state compared to other issued credit cards.

4. (original) The secure credit card of claim 2 wherein the first LFSR has a different configuration compared to other issued credit cards.

5. (original) The secure credit card of claim 2 wherein the first LFSR is configured to have a sequence length of 2^n-1, where n is a number of stages in the shift register.

6. (original) The secure credit card of claim 2 wherein the first LFSR has an initial state and configuration set by electronic fuses.

7. (original) The secure credit card of claim 1 wherein the pseudo-random bit sequence generator is a second linear feedback shift register (LFSR).

8. (original) The secure credit card of claim 7 wherein the second LFSR has a different initial state compared to other issued credit cards.

9. (original) The secure credit card of claim 7 wherein the second LFSR has a different configuration compared to other issued credit cards.

10. (original) The secure credit card of claim 7 wherein the second LFSR is configured to have a sequence length of 2^n-1, where n is a number of stages in the shift register.

11. (original) The secure credit card of claim 7 wherein the second LFSR has an initial state and configuration set by electronic fuses.

12. (original) The secure credit card of claim 1 wherein the clock drives the first counter and the second pseudo random bit generator for the same number of cycles.

13. (original) The secure credit card of claim 1 wherein the clock drives the first counter and the second pseudo random bit generator for numbers of cycles having a fixed mathematical relationship.

14. (cancelled)

15. (original) The secure credit card of claim 1 wherein the clock has a clock speed in the range of about 0.1-100 megahertz.

16. (original) The secure credit card of claim 1 wherein the first counter and second pseudo-random bit sequence generators are virtual entities emulated in an electronic processor.

17. (original) The secure credit card of claim 1 further comprising a display for displaying numbers produced by the first counter and the second pseudo random bit generator.

18. (original) The secure credit card of claim 1, further comprising a means for activating the card for a desired time duration.

19. (original) The secure credit card of claim 1, further comprising a means for activating the card for a desired number of transactions.

20. (original) The secure credit card of claim 1, further comprising a means for resetting a secure access code or PIN.

21. (currently amended) A secure credit card, comprising:

a) a virtually emulated first linear-feedback shift register (LFSR);

b) a second linear-feedback shift register (LFSR) or a second virtually emulated LFSR; and

c) a clock for driving the first and second linear-feedback shift registers, wherein the clock is operable for an unpredictable number of cycles, <u>wherein the unpredictable number of cycles is determined by a human action of unpredictable duration.</u>

22. (original) The secure credit card of claim 21 wherein the first LFSR and second LFSR have different initial states compared to other issued credit cards..

23. (original) The secure credit card of claim 21 wherein the first LFSR and second LFSR have different configurations compared to other issued credit cards..

24. (original) The secure credit card of claim 21 wherein the first LFSR and second LFSR are configured to have a sequence length of 2^n-1, where n is a number of shift register stages.

25. (original) The secure credit card of claim 21 wherein the first LFSR and second LFSR each have an initial state and configuration set by electronic fuses.

26. (original) The secure credit card of claim 21 wherein the clock drives the first LFSR and the second LFSR for the same number of cycles.

27. (original) The secure credit card of claim 21 wherein the clock drives the first LFSR and the second LFSR for numbers of cycles having a fixed mathematical relationship.

28. (cancelled)

29. (cancelled)

30. (original) A method for authenticating a secure credit card having a linear feedback shift register (LFSR), comprising the steps of:

a) sending from the credit card to a financial institution a card identification number uniquely associated with LFSR settings;

c) sending from the financial institution to the credit card a request for an output of the LFSR after m clock cycles;

d) operating the LFSR for m clock cycles to produce an LFSR output;

e) sending the LFSR output from the card to the financial institution;

f) comparing the LFSR output with LFSR settings for the credit card to authenticate the credit card.

31. (original) The method of claim 30 further comprising the step of looking up in a database at the financial institution the settings information associated with the card identification number.

32. (original) A method for authenticating a secure credit card having a counter and a pseudo-random bit sequence generator (GEN), comprising the steps of:

a) driving the counter and the GEN for numbers of cycles having a fixed or predictable mathematical relationship;

b) transmitting to a financial institution outputs of the counter and GEN after step (a);

c) authenticating the credit card by comparing the outputs produced in step (b) with settings of the counter and GEN known to the financial institution.

33. (original) The method of claim 32 wherein the counter and GEN are driven for the same number of cycles.

34. (original) The method of claim 32 wherein the unpredictable number of cycles is determined by a clock operated for an unpredictable duration.

35. (original) The method of claim 34 wherein the unpredictable duration is determined by a human action.

36. (new) The secure credit card of claim 1 wherein said unpredictable number of cycles is determined by a human action of unpredictable duration is determined by one of a duration a keypad is pressed, a duration between two keypad entries, or a duration between card activation and communication with a card reader.

37. (new) The method of claim 35 wherein said human action is determined by one of a duration a keypad is pressed, a duration between two keypad entries, or a duration between card activation and communication with a card reader.

38. (new) The method of claim 32 wherein in said driving step, said counter and GEN are each driven for a plurality of cycles.